secunet
monitor

Angriffserkennungs-system und Security-Monitoring

für Ihr Netzwerk

secunet.com

Angriffserkennung auch für das IT-Sicherheitsgesetz 2.0

Frühe Erkennung von Sicherheitsproblemen, wertvolle Daten für Forensik und Reaktion sowie verringerte Auditaufwände

Das im Mai 2021 verabschiedete IT-Sicherheitsgesetz 2.0, kurz IT-SiG 2.0, verpflichtet (unter anderem) KRITIS-Betreiber zum Einsatz von sogenannten Systemen zur Angriffserkennung, welche durch technische Werkzeuge und organisatorische Einbindung unterstützter Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme erfolgen muss. Der Einsatz solcher Systeme ist ab dem 1. Mai 2023 verpflichtend.

secunet bietet mit „secunet monitor“ ein solches Angriffserkennungssystem für den Bereich der kritischen Infrastrukturen nach aktuellem Stand der Technik an. KRITIS-Betreiber aus unterschiedlichen Sektoren setzen dieses System bereits seit mehreren Jahren ein. Das System weist dabei Sensorik in Netzwerken, z.B. im Netz der Leitstellenebene, auf und wertet die Kommunikation im Netzwerk hinsichtlich verschiedener Erkennungsfunktionen (Assets, Kommunikation untereinander, Schwachstellen, Anomalien und Hinweise auf versteckte Angriffe) aus. secunet monitor schützt dabei vor allem den IT/OT-Mischbetrieb und deckt mit den Sensoren nicht nur den internen IT- und OT-Bereich ab, sondern auch den Übergang IT-OT – denn viele Gefahren für das OT-Netz gehen aktuell vom angebundenen IT-Bereich aus.

Das IT-Sicherheitsgesetz 2.0 empfiehlt drei Maßnahmen zur Angriffserkennung: Abgleich mit statischen Mustern, generische Muster sowie Verfahren der künstlichen Intelligenz und die Erkennung von Abweichungen des störungsfreien Betriebs. secunet monitor bedient mit jeweils unabhängigen Erkennungsmodulen alle drei vorgeschlagenen Punkte durch die Verwendung von IOCs (Indicators Of Compromise; „bekannte Signaturen“), einer fortschrittlichen Angriffsdetektion mit Mustererkennung ohne Verwendung von IOCs und der Anomalieerkennung mit vorheriger Baseline-Erstellung. Damit werden die Anforderungen aus dem IT-SiG 2.0 erfüllt.

Tipp:

Die Lage der IT-Sicherheit in Deutschland 2021
BSI Lagebericht 2021

secunet monitor erkennt Lücken in Ihren Systemen – bevor und falls sie ausgenutzt werden

secunet monitor erweitert Ihre derzeitige Sicherheitsstruktur bzw. Ihr bestehendes System zur Angriffserkennung oder etabliert ein solches in Ihrer Infrastruktur. secunet monitor ist eine Software-Appliance mit passiven Sensoren, die den Netzwerkverkehr datenschutzkonform erfassen. Im zentralen System werden diese Daten analysiert, korreliert und erlernt.

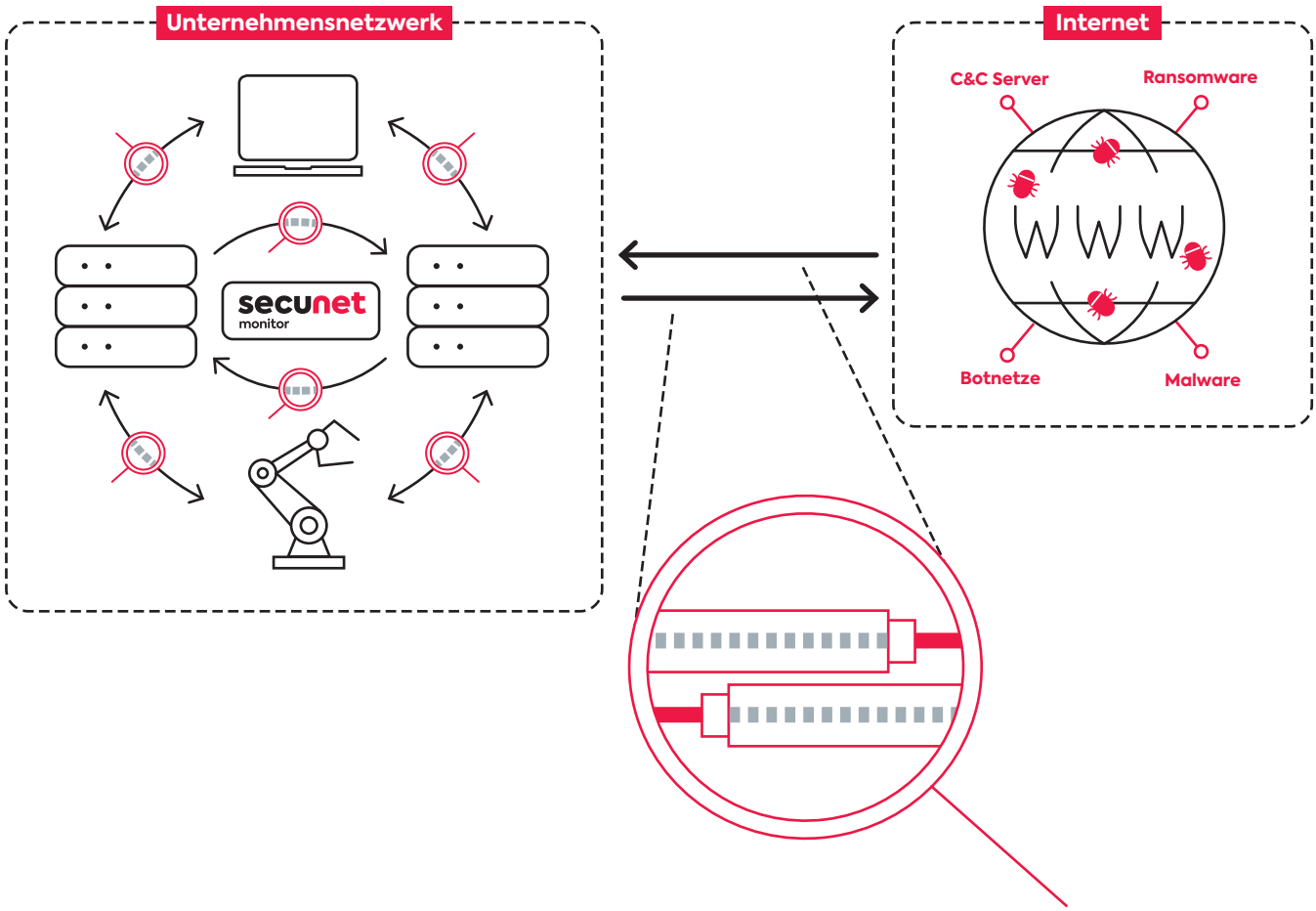
Das System selbst ist dadurch nicht erkennbar und standardmäßig rückwirkungsfrei, kann dadurch also auch keine negativen Effekte auf die überwachten Netzwerke und Geräte auslösen.

Vorteile auf einen Blick

Zielgerichtet
Beugt fortschrittlichen Angriffsformen vor und erkennt diese, ermöglicht eine dynamische Aufdeckung von Verhaltensänderungen und stärkt die Proaktivität sowie die Netzwerkresistenz

Komfortabel
Bietet eine intuitive aber dennoch tiefgehende Web-Oberfläche, operationalisiert nächste Schritte durch Empfehlungen und ist automatisierbar über eine REST API

Premiumsicher
Erkennt auch sehr unauffällige Sicherheitsprobleme, geht selbst nur passiv vor und ermöglicht eine Datenschutz-konforme Auswertung

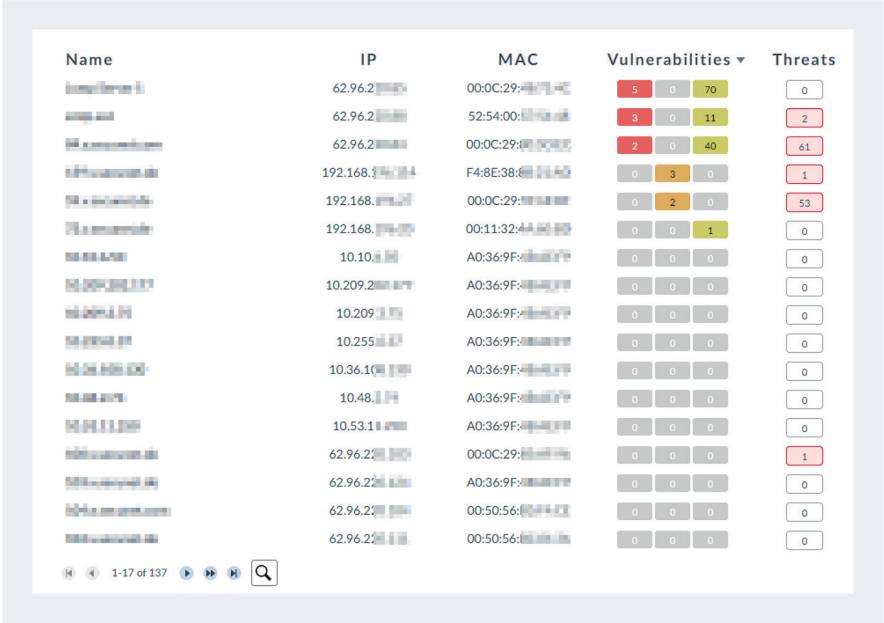


Netzwerk-Sicherheits-überwachung als modulares System

secunet monitor ist unsere Lösung für Ihren Bedarf an Network Security Monitoring (NSM) und Ihr System zur Angriffserkennung im Netzwerk. monitor überwacht die Abläufe und „Systeme“ in Ihren Netzen auf Aktivitäten oder Zustände die nicht so sind, wie sie sein sollten. monitor nutzt passive Netzwerkverkehrsanalysen (siehe Funktionsweise) um Assets, Schwachstellen, Compliance-Abweichungen, mögliche Angriffe und Anomalien zu erkennen.

Mit diesen Modulen zur Sicherheit im Netzwerk

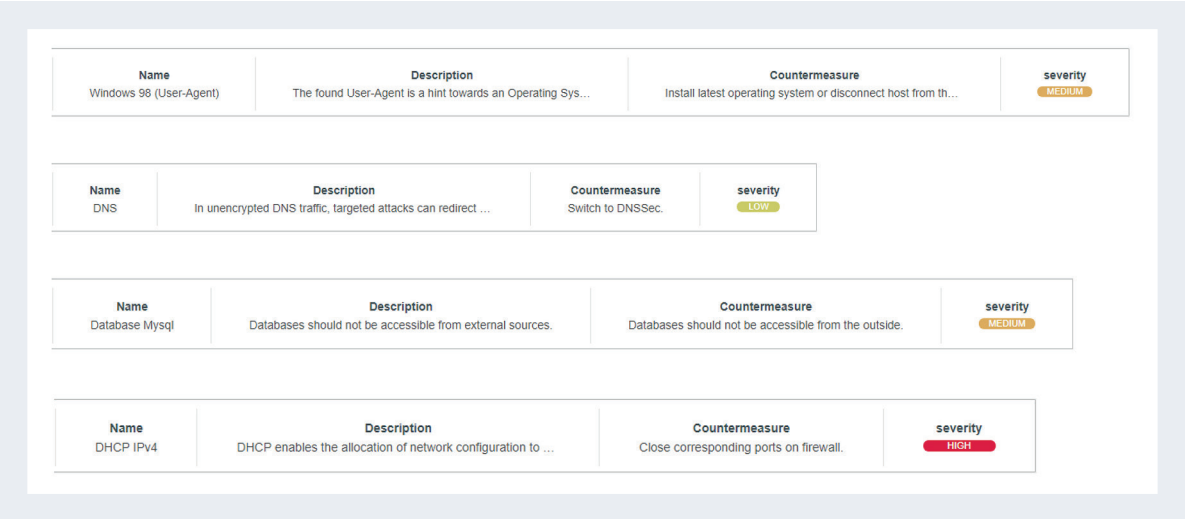
Assets aufspüren



Zur Erkennung und Überwachung und zur Aufdeckung von unbekannten Angriffen extrahiert monitor Kommunikationspartner aus dem Netzwerkverkehr und konsolidiert diese als Assets.

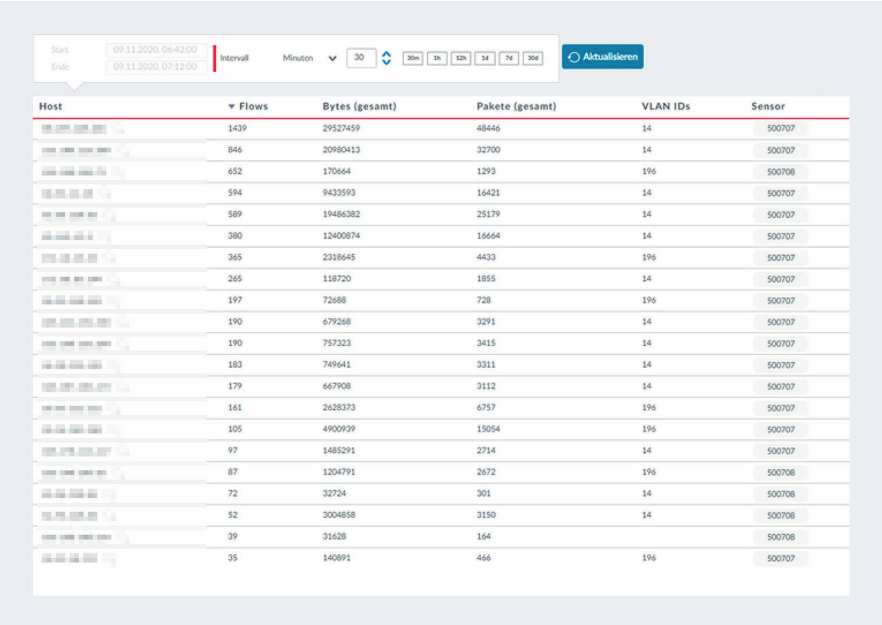
Automatisch erstellte Profile und individuell gepflegte Details ermöglichen eine zielgenaue Verortung von Auffälligkeiten und machen unerwünschte Gäste sichtbar.

Schwachstellen aufdecken



Um Lücken im bestehenden Vorgehen zu erkennen und um Probleme aufzudecken, die unbekannt sind, analysiert secunet monitor den Netzwerkverkehr auf Schwachstellen wie z. B. veraltete Betriebssysteme. Neben einer Qualitätssicherung für das Schwachstellenmanagement senkt dies das Risiko von versteckten Abwehrschwächen.

Compliance verifizieren



Zustände oder Aktivitäten, die nicht den Vorgaben entsprechen oder bei denen sich Schwachstellen ergeben, können über vordefinierte, aber auch individuell anpassbare Compliance-Regeln erkannt und eingegrenzt werden. Das intuitive Standardregelset und der Network Policy Editor ermöglichen eine Qualitätskontrolle für Sicherheitsmaßnahmen und eine Benachrichtigung von Compliance-Verstößen oder unerwartetem Verhalten.

Angriffe erkennen

severity	history	first occurrence	last occurrence	Amount	Type	classification
HIGH		14.12. • 16:14:02	14.12. • 16:38:02	8	UDP	HIDDEN DNS SUB DOMAIN TUNNEL
HIGH		14.12. • 16:28:02	14.12. • 16:31:02	2	ICMPv4	ICMPV4 TUNNEL TEXT
HIGH		14.12. • 16:16:02	14.12. • 16:37:02	3	TCP	POSSIBLE QUANTUM INSERT
HIGH		14.12. • 16:13:02	14.12. • 16:38:32	3	UDP	HIDDEN DNS SUB DOMAIN TUNNEL
HIGH		14.12. • 16:12:02	14.12. • 16:39:32	5	TCP	HTTP IMAGE REQUESTED AND OCTET STREAM DELIVERED
MEDIUM		14.12. • 16:23:02	14.12. • 16:33:32	2	TCP	SUSPICIOUS REQUESTS WITH SAME PATH TO DIFFERENT HOSTS
MEDIUM		14.12. • 16:21:02	14.12. • 16:34:32	2	TCP	RDP CONNECTION
MEDIUM		14.12. • 16:20:02	14.12. • 16:20:02	1	TCP	SOCKSV4A CONNECTION
MEDIUM		14.12. • 16:35:02	14.12. • 16:35:02	1	TCP	SOCKSV4A CONNECTION
LOW		14.12. • 16:27:02	14.12. • 16:31:32	2	UDP	FAILED DNS RESOLVING TO POSSIBLE DGA BASE DOMAIN OA4YSOBQ
LOW		14.12. • 16:26:02	14.12. • 16:32:02	2	UDP	FAILED DNS RESOLVING TO POSSIBLE DGA BASE DOMAIN BAR JGVR
LOW		14.12. • 16:25:02	14.12. • 16:32:32	2	TCP	HTTP GET CONNECTION TO POSSIBLE DGA BASE DOMAIN OTZP1WLI
LOW		14.12. • 16:24:02	14.12. • 16:33:02	2	UDP	FAILED DNS RESOLVING TO POSSIBLE DGA BASE DOMAIN TUGDRUXW
LOW		14.12. • 16:22:02	14.12. • 16:34:02	2	TCP	HTTP GET CONNECTION TO POSSIBLE DGA BASE DOMAIN YXM2SUGZ
LOW		14.12. • 16:19:02	14.12. • 16:35:32	2	TCP	CONNECTION TO TOR NODE
LOW		14.12. • 16:18:02	14.12. • 16:36:02	2	TCP	CONNECTION TO TOR NODE
LOW		14.12. • 16:17:02	14.12. • 16:36:32	3	TCP	CONNECTION TO TOR EXIT NODE

Zur Erkennung und Analyse von Angriffen, die von automatisierten Scans über Schadsoftware bis zu gezielten und hochkomplexen Angreiferaktivitäten reichen können, extrahiert monitor Indikatoren aus dem Netzwerkverkehr. Regelwerke, Heuristiken und maschinelles Lernen ermöglichen eine schnellere Erkennung sowie eine Zweitmeinung bei anderen Signalen wie z. B. Auffälligkeiten auf Endpunkten und bieten so eine Chance, fortschrittliche Angriffe frühzeitig einzufangen.

Anomalien entdecken

Neben je nach Signalstärke relativ eindeutigen Indikatoren können sich Sicherheitsprobleme auch im Grundrauschen verstecken. Monitor erkennt daher Anomalien im Netzwerkverkehr bzw. -verhalten, die auf Konfigurationsprobleme, Fehler oder aber auch Angriffe hindeuten können. Mittels Verhaltensanalyse und durch Machine Learning automatisch erstellte Baselines wird auf Anomalien hingewiesen.

Mit secunet monitor stärken Sie Ihre Resistenz und Resilienz gegen Angriffe und andere Sicherheitsprobleme.

Das Produkt in der Praxis (Umsetzungsbeispiel)

Moderne Netzwerke haben komplexe Strukturen und damit viele mögliche Punkte, an denen sicherheitsrelevante Daten vorbeifließen. Der größte Teil wird jedoch weiterhin über zentrale Knotenpunkte abgewickelt – z. B. an Netzübergängen. Um auch weitere relevante Punkte und Bereiche abzudecken, bietet secunet monitor Möglichkeiten für einen verteilten Datenabgriff vom Netzwerkknoten bis hin zu individuellen Systemen bzw. Maschinen.

Kontinuierliche Datenaufnahme
(Sensor)

Intelligente Auswertung
(Kernsystem)

Intuitive Darstellung
(Webanwendung – lokal oder „as-a-Service“)

Die Sensor-Komponente greift Metadaten und verdächtige Inhalte ab und sendet sie an ein zentrales Kernsystem. Auf diesem laufen u. a. mitlernende Algorithmen zur Erkennung von Anomalien. Über die Webanwendung (verfügbar rein lokal bei Ihnen als On-Premises oder aus unserer sicheren Cloud als as-a-Service heraus) sind Analysen und Handlungsempfehlungen annährend in Echtzeit auswertbar.

Mit secunet monitor können Sie einige spezialisierte Sicherheitsprodukte ersetzen oder ergänzen. So können Sie sich zukünftig auf die Lösung von Problemen konzentrieren und sich selbst, Ihren Kollegen oder Ihren Mitarbeitern ermöglichen, die Sicherheit der Organisation nachhaltig und messbar zu steigern.

Stark im produktionsnahen IT/OT-Mischbetrieb

Wie wollen Sie unsere Lösung nutzen?
Es gibt mehrere Möglichkeiten, secunet monitor in Ihre bestehende IT-Infrastruktur zu integrieren. Wir beraten Sie gerne und entwerfen mit Ihnen gemeinsam die beste Strategie für Ihre Organisation.

as-a-Service

- Sensorik vor Ort, Kernsystem in einer gesicherten Umgebung bei secunet
- Einfachste Integration und schmalere Infrastruktur
- Flexible Nutzung und weniger Administrationsaufwände

In diesem Modell können alle Auswertungen im secunet-Rechenzentrum bzw. der secunet Cloud über sichere Verbindungen und auf sicherer Infrastruktur durchgeführt werden. Für allerhöchste Sicherheit ist eine optionale Anbindung über secunet SINA möglich.

On-Premises

- Volle Kontrolle und Datenverbleib im eigenen Netz
- Firmeninterne Anbindung
- Auf Wunsch Unterstützung durch secunet oder Partner über sichere Fernzugänge

Alle notwendigen Komponenten von Sensorik über Kernsystem bis Webanwendung werden bei Ihnen lokal vor Ort integriert und betrieben. secunet oder einer unserer spezialisierten und vertrauenswürdigen Partner übernimmt im Anschluss an eine Konzeptionsphase auf Wunsch die Auswahl und Integration der Infrastruktur.

Managed Service durch Partner

- Integration, Betrieb und Bedienung durch kompetente Partner
- Sowohl mit secunet monitor On-Premises, als auch secunet monitor as-a-Service möglich
- Skalierungseffekte und Expertise durch spezialisierte Dienstleister

Auf Wunsch wird secunet monitor durch Partner von secunet integriert, betrieben und bedient. Je nach Betriebsmodell sind auch Teilprozesse als Managed Service möglich – z. B. der Betrieb durch einen Dienstleister und die Bedienung durch interne Mitarbeiter.

secunet – Schutz für digitale Infrastrukturen

secunet ist Deutschlands führendes Cybersecurity-Unternehmen. In einer zunehmend vernetzten Welt sorgt das Unternehmen mit der Kombination aus Produkten und Beratung für widerstandsfähige, digitale Infrastrukturen und den höchstmöglichen Schutz für Daten, Anwendungen und digitale Identitäten. secunet ist dabei spezialisiert auf Bereiche, in denen es besondere Anforderungen an die Sicherheit gibt – wie z. B. Cloud, IIoT, eGovernment und eHealth. Mit den Sicherheitslösungen von secunet können Unternehmen höchste Sicherheitsstandards in Digitalisierungsprojekten einhalten und damit ihre digitale Transformation vorantreiben.

Über 700 Expert*innen stärken die digitale Souveränität von Regierungen, Unternehmen und der Gesellschaft. Zu den Kunden zählen die Bundesministerien, mehr als 20 DAX-Konzerne sowie weitere nationale und internationale Organisationen. Das Unternehmen wurde 1997 gegründet. Es ist im Segment Prime Standard der Frankfurter Wertpapierbörse gelistet und erzielte 2020 einen Umsatz von 285,6 Mio. Euro (vorläufige Geschäftsergebnisse, Stand: 22. Januar 2021).

secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit.

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com